

Amendments to the Claims

Please amend the claims in the manner indicated.

1. (original) An apparatus, comprising:

a hash circuit to receive first and second input values for a current hash stage and

to generate an output value from the current hash stage based on the first

and second input values;

a numerical sequencer coupled to the hash circuit to generate a sequence of

numbers during the current hash stage and to provide at least a portion of a

current one of the sequence of numbers as the first input value for a

subsequent hash stage;

a feedback circuit coupled to the hash circuit to provide at least a portion of the

output value as the second input value for the subsequent hash stage; and

a control circuit coupled to the numerical sequencer to stop generating the

sequence of numbers upon an occurrence of a first predetermined event

and to resume generating the sequence of numbers upon an occurrence of

a second predetermined event.

2. (original) The apparatus of claim 1, wherein:

the hash circuit is to receive the first and second input values at a beginning of the

current hash stage.

3. (original) The apparatus of claim 1, wherein:
the first predetermined event includes receipt of a request for a pseudo-random
number.
4. (original) The apparatus of claim 1, wherein:
the second predetermined event includes a part of the subsequent hash stage.
5. (original) The apparatus of claim 1, wherein:
the second predetermined event includes a beginning of the subsequent hash
stage.
6. (original) The apparatus of claim 1, wherein:
The numerical sequencer includes a counter.
7. (original) The apparatus of claim 1, wherein:
the numerical sequencer includes a linear feedback shift register.
8. (original) The apparatus of claim 1, wherein:
said at least a portion of the current one of the sequence of numbers includes
predetermined bits of the current one of the sequence of numbers.

9. (original) The apparatus of claim 1, wherein:
said at least a portion of the output value includes predetermined bits of the output value.
10. (original) A system, comprising:
a processor;
a memory coupled to the processor; and
a pseudo-random number generator coupled to the processor and including:
a hash circuit to receive first and second input values for a current hash stage and to generate an output value from the current hash stage based on the first and second input values;
a numerical sequencer coupled to the hash circuit to generate a sequence of numbers during the current hash stage and to provide at least a portion of a current one of the sequence of numbers as the first input value for a subsequent hash stage;
a feedback circuit coupled to the hash circuit to provide at least a portion of the output value as the second input value for the subsequent hash stage; and
a control circuit coupled to the numerical sequencer to stop generating the sequence of numbers upon an occurrence of a first predetermined event and to resume generating the sequence of numbers upon an occurrence of a second predetermined event.

11. (original) The system of claim 10, wherein:
the hash circuit is to receive the first and second input values at a beginning of the
current hash stage.
12. (original) The system of claim 10, wherein:
the first predetermined event includes receipt of a request for a pseudo-random
number.
13. (original) The system of claim 10, wherein:
the second predetermined event includes a part of the subsequent hash stage.
14. (original) The system of claim 10, wherein:
the second predetermined event includes a beginning of the subsequent hash
stage.
15. (original) The system of claim 10, wherein:
The numerical sequencer includes a counter.
16. (original) The system of claim 10, wherein:
the numerical sequencer includes a linear feedback shift register.

17. (original) The system of claim 10, wherein:
said at least a portion of the current one of the sequence of numbers includes
predetermined bits of the current one of the sequence of numbers.
18. (original) The system of claim 10, wherein:
said at least a portion of the output value includes predetermined bits of the output
value.
19. (currently amended) A method, comprising:
generating a series of values with a numerical sequencer during each of a previous
hash stage, a current hash stage, and a subsequent hash stage;
receiving one of the values as a first hash input;
receiving a hash output from the previous hash stage as a second hash input;
hashing the first and second hash inputs during a current hash stage to produce a
current hash output;
stopping the generating when a first predetermined event occurs and restarting the
generating when a second predetermined event occurs, if the first
predetermined event occurs during the current hash stage; and
continuing the generating during the current hash stage, if the first predetermined
event does not occur during the current hash stage.

20. (original) The method of claim 19, wherein:
the first predetermined event includes receiving a request for a pseudo-random
number.
21. (original) The method of claim 19, wherein:
the second predetermined event includes a beginning of the subsequent hash
stage.
22. (currently amended) A machine-readable medium having stored thereon
instructions, which when executed by at least one processor cause said at least one
processor to perform operations comprising:
generating a series of values with a numerical sequencer during each of a previous
hash stage, a current hash stage, and a subsequent hash stage;
receiving one of the values as a first hash input;
receiving a hash output from the previous hash stage as a second hash input;
hashing the first and second hash inputs during a current hash stage to produce a
current hash output;
stopping the generating when the first predetermined event occurs and restarting
the generating when a second predetermined event occurs, if a first
predetermined event occurs during the current hash stage; and
continuing the generating if the first predetermined event does not occur during
the current hash stage.

23. (original) The medium of claim 22, wherein:

the first predetermined event includes a request for a pseudo-random number.

24. (original) The medium of claim 22, wherein:

the second predetermined event includes a beginning of a subsequent hash stage.